



Administrative Tribunal

Distr. Limited
28 September 2007

Original: French

ADMINISTRATIVE TRIBUNAL

Judgement No. 1321

Case No. 1395

Against: The Secretary-General
of the United Nations

THE ADMINISTRATIVE TRIBUNAL OF THE UNITED NATIONS,
Composed of Mr. Spyridon Flogaitis, President; Mr. Dayendra Sena Wijewardane, Vice-President;
Ms. Brigitte Stern;

Whereas at the request of a former staff member of the International Criminal Tribunal for the former Yugoslavia (ICTY), the President of the Tribunal granted an extension of the time limit for filing an application with the Tribunal until 31 July 2004 and twice thereafter until 31 January 2005;

Whereas, on 11 January 2005, the Applicant filed an Application requesting the Tribunal:

“4. to order:

That the Applicant be reinstated;

That the Applicant be paid three years base salary for denial of due process;

That the Applicant may be paid three years base salary in lieu of reinstatement.”

Whereas at the request of the Respondent, the President of the Tribunal granted an extension of the time limit for filing a Respondent’s answer until 31 July 2005 and once thereafter until 16 September 2005;

Whereas the Respondent filed his Answer on 15 September 2005;

Whereas the Applicant filed Written Observations on 22 December 2005;

Whereas, on 21 November 2006, the Tribunal decided to postpone consideration of this case until its next session;

Whereas the statement of facts, including the employment record, contained in the report of the Joint Disciplinary Committee (JDC) reads, in part, as follows:

“Employment History

... On 10 April 2000, [the Applicant] joined the International Criminal Court for the former Yugoslavia (ICTY), The Hague, as a Security Officer for an initial period of three months. His contract was subsequently renewed for one year and then for another to carry him through 9 July 2002. His current two-year contract at the G-3 level is to expire on 9 July 2004. He has been placed on suspension with full pay since 6 May 2003.

Background leading to the charges

... The misconduct allegedly occurred at ICTY on 7 March 2003. According to the report from ICTY, the Information Technology Services Section (ITSS) of ICTY received a network report indicating that an anti-virus scanner [...] has identified the presence of two known hostile network tools [...] and 15 attempts to use them from two separate computer terminals between 3:06 a.m. and 5:51 a.m., on the morning of 7 March 2003 to gain access into the ICTY Registry electronic network. Nonetheless, the said attempts were not successful and caused no damage to the ICTY information system. The user login name for all the attempts [corresponded with the Applicant’s, who was on night shift duty as a Security Officer at the relevant time].

... Authorisation was issued to investigate those incidents. As a precaution, the ICTY Administration locked [the Applicant]’s internet account on 7 March 2003.

... On 14 March 2003, a meeting took place between [the] Chief of Security, ICTY, [...] an Associate Information Security Officer, ICTY, and [the Applicant]. According to [the Chief of Security], he and [the Associate Information Security Officer] asked [the Applicant] questions about his most recent activities in connection with network tools. [The Applicant] allegedly replied that he had used network tools ‘one or two months ago’. When he was showed the ITTS network report [the Applicant] stated that he had used his own CD-ROM, on 7 March 2003, but denied having used the tools identified in the network report. Again, according to [the Chief of Security],

‘[the Applicant] was given numerous opportunities to indicate that he had been using personal software on the ICTY system or taken any other action which might, in any way, be construed as inappropriate. Only after he had, for whatever reason, failed to respond to these opportunities was he shown the technical report indicating the UNEQUIVOCAL link to his user ID and the unauthorized attempts to gain access.’

[The Chief of Security] emphasized that at no stage was [the Applicant] subject to hostile or intimidating questioning or threatened with disciplinary action’.

... At the request of [the Chief of Security], [the Applicant] returned to his residence, retrieved 10 CD-ROMs and brought them to ICTY. ... According to [the Chief of Security], [the Applicant] had used several of those CD-ROMs, but was not sure which one may have the ITTS network report. [The Chief of Security] stated that

‘[a]ll the CD-ROMs were introduced into the network but none had automated capability (“self booting”) and could not have caused the reported activity just by insertion into the computer. [The Associate Information Security Officer] then attempted to copy tools to the hard drive. The copy process was halted by the system when [one of the two hostile network tools] was encountered and ITTS informed [him] that the same report has been generated.’

... In a fax dated 28 March 2003 to [the Office for Human Resources and Management (OHRM)], [the] Acting Chief of Administration, ICTY, reported [the Applicant]'s case with a recommendation that [the Applicant] be suspended from duty 'based on the vital need to keep secure the information of the ICTY'.

... In a memorandum dated 2 May 2003, [OHRM] sent [the Applicant] the charge against him ... [He was asked] to respond to the allegations of misconduct and advised ... of the availability of the assistance of the Panel of Counsel. [He was] also informed that he would be placed on suspension with full pay ... effective 6 May 2003 ...

... [On] ... 20 May 2003, [the Applicant] provided his response. ... He claimed that there existed numerous inconsistencies in the documents which formed part of the allegations of misconduct. He stated that 'it was never my intention to do any harm to the ICTY network. ...'

... In a memorandum dated 26 August 2003, [OHRM] referred [the Applicant]'s case to the JDC in New York ...

On 5 February 2004, the JDC submitted its report. Its considerations, conclusions and recommendation read as follows:

“Considerations

...

31. ... The Panel observed ... that there is no provision in [administration instruction entitled 'IT Guidelines' (ICTY/AI/2003/03) dated 7 February 2003] concerning the use of office computers to view or browse personal materials when an ICTY staff member is not on active duty, as in the present case.

...

34. What is at issue is whether [the Applicant] tried to run the hacker software himself or whether the anti-virus software detected it passively. The Panel heard conflicting evidence from witnesses. ...

...

36. The Panel heard evidence from [the Applicant's] supervisors. Everyone testified that he had been a solid performer with a completely satisfactory track record. He had given none of his supervisors any reason to question either his integrity or his performance. ...

...

38. The Panel heard evidence from [the Applicant's] counsel that there may have been other motivations in bringing charges against him. It found no evidence of this, but is convinced that the charges were brought against [the Applicant] because ICTY and the Administration felt that he had tried to deploy well-known hacker software against the network.

39. The central question then is whether [the Applicant] tried to activate the hacker software himself. ...

40. In the face of the conflicting evidence, the Committee finds it hard to make a finding on [the Applicant's] culpability. His background as a telecommunications engineer and his professed interest in IT matters should have alerted him to the possibility that bringing CD-ROMs with hacker software into the network could create difficulties.

41. However, in the Panel's view, the evidence presented by the Administration is not adequate and leaves room to doubt that [the Applicant] tried to introduce hacker software into the network or to gain access to any database.

Conclusions and recommendations

42. The Panel thus concludes that the [Applicant's] action does not amount to misconduct, but that he showed poor judgment in introducing his own CDs into ICTY network.

43. The Panel therefore *unanimously recommends* that the [Applicant] receive a reprimand for his actions. It does not, however, believe that more serious disciplinary action would be warranted. ...”

On 5 February 2003, the Under-Secretary-General for Management transmitted a copy of the JDC report to the Applicant and informed him as follows:

“The Secretary-General ... does not share the JDC's conclusion that your actions did not amount to misconduct and he regrets that he also cannot agree with the JDC's assessment of the evidence against you. He considers that the dispositive issue in this case is that you, a telecommunications engineer by background, introduced into the ICTY network your CD-ROMs even though you knew that they contained hacker software designed to attack the network. It is far less important whether or not you tried to run the hacker tools, notwithstanding the confirmation by the manufacturer - not just any expert - of the antivirus software that you must have tried to launch or copy the hacker software for the anti-virus to be activated. The Secretary-General considers that the fact alone that you introduced into the ICTY's network hacker software and you knew what those tools could do to the Organization's network leaves no doubt as to your culpability and has eroded the Organization's trust in you.

As a result, the Secretary-General considers that your conduct amounted to a serious violation of the standards of conduct and integrity expected of staff members of the Organization, and that this misconduct is incompatible with your continued service with the Organization. In view of the seriousness of your misconduct, the Secretary-General has decided not to accept the JDC's recommendation that you should be reprimanded. Pursuant to his discretionary authority to impose appropriate disciplinary measures, the Secretary-General has decided to separate you from service with compensation in lieu of notice pursuant to staff rule 110.3 (a) (vii), with effect from close of business on the day you receive this letter.”

On 11 January 2005, the Applicant filed the above-referenced Application with the Tribunal.

Whereas the Applicant's principal contentions are:

1. He was denied due process.
 2. He was not treated with fairness by the ICTY Administration, as required by staff regulation 1.2
- (b).
3. He was not accorded fair and equitable treatment during the disciplinary proceedings.

Whereas the Respondent's principal contentions are:

1. The Secretary-General has broad discretion with regard to disciplinary matters, and this includes determination of what constitutes serious misconduct warranting separation from service.
2. The Applicant failed to meet the standards of conduct required of an international civil servant and the disciplinary measure imposed was proportionate to the misconduct.

3. The Applicant was afforded due process and was treated fairly.

The Tribunal, having deliberated from 30 October to 21 November 2006, in New York, and from 25 June to 27 July 2007, in Geneva, now pronounces the following Judgement:

I. The Applicant joined the service of ICTY as a Security Officer on 10 April 2000. His position encompassed various security functions: security of judges and detainees, and the safety of field missions in the former Yugoslavia. Before joining ICTY, he had worked in telecommunications as a Systems and Telecommunications Engineer from 1997 to 2000. Prior to the events which prompted this case, his performance was consistently highly rated by his supervisors.

II. The incident leading to the dismissal, which the Applicant is contesting before the Tribunal, relates to the integrity of the ICTY Information Technology network. This system is complex, as evidenced by an internal ICTY note dated 31 March 2003:

“The ICTY has a computer network, which consist of about 1400 computers and servers, covering a geographical area including four buildings in the metropolitan area of The Hague as well as the six field offices in the region of the former Yugoslavia. This network is a collection of computers, which holds critical organisational data and facilitates the daily work of nearly all ICTY staff.”

The system is, however, not just complex: it is, above all, extremely sensitive, as it contains personal information, the confidentiality of which is imperative. The information in the ICTY network includes, specifically, the personal details of victims, witnesses and accused persons, information which must not be publicly accessible. Any unauthorized intrusion into the system could have extremely serious consequences, putting witnesses' lives at risk, for example. This issue is also highlighted in several internal memoranda:

“The ICTY computer system contains very large amounts of highly sensitive material. This includes, to cite three obviously examples of information, which may only be seen by those authorised to do so, the personal details of witnesses who may be under threat of death, pending legal decisions, and secret plans for the arrest of alleged war criminals.

... ICTY is concerned with prosecuting war criminals, and our information assets include evidentiary material, court records and confidential witness information. Breach of these records, could result in compromised court cases, loss of legal and historical records, and the putting in jeopardy of witnesses to serious crimes ... Attack and compromise of those systems poses very serious threats to the very work of the Tribunal, including the successful outcomes of war crimes cases, financial accountability, staff member confidentiality and the lives of the victims and witnesses.”

The Tribunal has emphasized the highly distinctive nature of the ICTY network, in order that the setting in which the Applicant was dismissed can be properly understood.

III. The dispute relates not to the facts leading to the Applicant's dismissal, but to the interpretation thereof. During the night of 7 March 2003, the Applicant used personal CD-ROMs containing hacker software - PWS-Qwak

and Orifice 2000 - several times (at least seven and, possibly, as many as fifteen) on two different computers on the ICTY premises. In doing so, he set off a computer alert.

IV. It is not entirely clear how to interpret his actions. The Applicant says he simply wanted to see, during his breaks, what was on his personal CD-ROMs, and that he had no intention of running the hacker software; the Administration asserts, on the contrary, that technical data on the computer logs in its possession indicate that the Applicant tried to copy the hacker programmes and use them on the ICTY network. The differing interpretations stem essentially from the fact that it cannot be ascertained what action triggered the computer alert. Some experts have attested that the anti-virus programmes installed on the ICTY network were capable of detecting passive hacker software, i.e. programs that were not running, while others, having conducted tests, argue that the alert could be triggered only by a hacker program that was running, i.e. being used to penetrate the network.

V. The Applicant was suspended with full pay on 6 May 2003. The JDC submitted a report on 5 February 2004 concluding that the Applicant's actions should not be regarded as misconduct but, at worst, poor judgement, and recommended a reprimand but no more serious disciplinary action. The Secretary-General did not accept the JDC's recommendation, finding that the Applicant was guilty of misconduct warranting dismissal pursuant to staff rule 110.3 (a) (vii). This decision was communicated to the Applicant on 5 February, and his dismissal, with compensation in lieu of notice, took effect on 17 February.

VI. The Applicant argues that the Administration construed ambiguous reports as evidence of harmful intent when no actual evidence of such intent has ever been entered. The Applicant does not challenge the discretionary authority of the Secretary-General, but contends that the Administration's statements give a false impression of his actions. The decision to dismiss him was thus inappropriate and violated his rights of due process. The Applicant therefore seeks:

- Reinstatement;
- Payment of three years' net base salary for denial of due process; and,
- Payment of three years' net base salary in compensation if he is not reinstated.

VII. According to the Administration, under the provisions of Article 101, paragraph 1, of the United Nations Charter, the Secretary-General has discretion to appoint staff and to ascertain whether they meet the criteria of efficiency, competence and integrity. The Tribunal has frequently upheld this approach (see Judgements No. 834, *Kumar* (1997) and No. 1245 (2005)). The Secretary-General has the discretionary authority to decide on appropriate disciplinary action or to dismiss staff members in the event of serious misconduct. He also has the authority to determine what constitutes serious misconduct and the scope of the disciplinary action to be taken.

VIII. In the present case, the Administration contends that the Applicant breached the standard of conduct expected of a United Nations staff member, and the disciplinary action taken was proportionate. Staff regulation 1.2 (b) and (f) require staff members to conduct themselves in a manner befitting their status and not to engage in any activity incompatible therewith. Prior to serving as a Security Officer at ICTY, the Applicant had trained as a computer engineer: he willfully inserted a CD-ROM containing hacker software into the ICTY network. The ICTY network contains vital confidential information on matters including the identity of victims and witnesses, as mentioned above, which must not be threatened in any way. Even if the Applicant's conduct had resulted in no harm, one must take into account the nature of his conduct, not the severity of its consequences. According to the Respondent, the mere fact of inserting the CD-ROM was, thus, improper.

IX. The Tribunal wishes to affirm, once again, that it is within the discretionary authority of the Secretary-General to decide whether a staff member has met the standards of conduct laid down in the Charter and the Staff Regulations & Rules. In its jurisprudence, the Tribunal has consistently permitted the Secretary-General broad latitude in disciplinary matters (see Judgements No. 424, *Ying* (1988); No. 425, *Bruzual* (1988); No. 479, *Caine* (1990); No. 515, *Khan* (1991); and No. 542, *Pennacchi* (1991).) In exercising such discretion, the Secretary-General must act without prejudice or other improper motive and respect the requirements of proper procedure (see Judgements No. 436, *Wield* (1988) and No. 641, *Farid* (1994)), as was made particularly clear in Judgement No. 941, *Kiwanuka* (1999):

“III. ... [I]n keeping with the relevant general principles of law, in disciplinary cases the Tribunal generally examines (i) whether the facts on which the disciplinary measures were based have been established; (ii) whether the established facts legally amount to misconduct or serious misconduct; (iii) whether there has been any substantive irregularity (e.g. omission of facts or consideration of irrelevant facts); (iv) whether there has been any procedural irregularity; (v) whether there was an improper motive or abuse of purpose; (vi) whether the sanction is legal; (vii) whether the sanction imposed was disproportionate to the offence; (viii) and, as in the case of discretionary powers in general, whether there has been arbitrariness. This listing is not intended to be exhaustive. Most recently in Judgement No. 898, *Uggla*, paragraph II (1998), the Tribunal made a similar general statement.

IV. Clearly the Tribunal takes the view that the imposition of disciplinary sanctions involves the exercise of a discretionary power by the Administration. It further recognizes that, unlike other discretionary powers, such as transferring and terminating services, it is also a special exercise of quasi-judicial power. For these reasons the process of review exercised by the Tribunal is of a particular nature. The Administration's interest in maintaining high standards of conduct and thus protecting itself must be reconciled with the interest of staff in being assured that they are not penalized unfairly or arbitrarily.”

X. Consistent with this approach, the Tribunal first observes that the facts are established and are not contested by the parties. The undisputed facts of the night of 7 March 2003, between 3.06 and 5.51 a.m., were summarized by the JDC as follows:

“The Panel has considered the evidence before it. A large number of facts are not in dispute. [The Applicant] acknowledges that not only was he on duty on 7 March 2003, but also he used two computer terminals during his break periods. [The Applicant] also acknowledges that he brought two CD-ROMs from his private collection and that he inserted those media into the ICTY's IT network. [The Applicant] further

acknowledges the presence of PWS-Qwak and Orifice 2000 on the CD-ROMs together with a very large number of other private files and folders.”

XI. Secondly, the Tribunal must consider whether the established facts legally amount to misconduct or serious misconduct. The ICTY administration considered the Applicant guilty of an illicit and dangerous act and forwarded the matter to OHRM in New York, as a breach of staff regulation 1.2 (b): “Staff members shall uphold the highest standards of efficiency, competence and integrity. The concept of integrity includes, but is not limited to, probity, impartiality, fairness, honesty and truthfulness in all matters affecting their work and status.” And staff regulation 1.2 (f):

“While staff members’ personal views and convictions, including their political and religious convictions, remain inviolable, staff members shall ensure that those views and convictions do not adversely affect their official duties or the interests of the United Nations. They shall conduct themselves at all times in the manner befitting their status as international civil servants and shall not engage in any activity that is incompatible with the proper discharge of their duties with the United Nations. They shall avoid any action and, in particular, any kind of public pronouncement that may adversely reflect on their status, or on the integrity, independence and impartiality that are required by that status.”

XII. The JDC did, it is true, regard the incidents of the night of 7 March 2003 more as a matter of negligence than of misconduct, stressing the lack of evidence put forward by the Administration to show harmful intent on the part of the Applicant. The Tribunal finds this line of argument unconvincing, however, finding that in some circumstances there can be misconduct even absent harmful intent.

XIII. The Tribunal has not been persuaded that the Applicant’s behavior did not amount to wrongdoing. An important element leading the Tribunal to this conclusion is that, when summoned shortly after the computer alert, the Applicant did not volunteer that he had been using personal CD-ROMs and admitted to the fact only upon being shown the relevant computer logs, as the JDC report indicates :

“On behalf of the Administration ... [the Respondent] recalled that [the Applicant], whose responsibilities as a Security Officer bore no relation to computer network, made 15 attempted use of his home made software containing known hacking tools, and that subsequent to the incident [the Applicant] did not come forward until after he was confronted with the anti-virus log report.”

In accordance with UNAT jurisprudence, the Applicant ought to have offered satisfactory explanations for his behaviour, but did not do so. (See Judgement No. 850, *Patel* (1997).)

XIV. Moreover, the Tribunal is of the opinion that, whether or not there was any harmful intent, the Applicant’s actions can correctly be regarded as wrongdoing in the circumstances of this case. Whether or not he tried to access and run the two programs, PWS-Qwak and Orifice2K, it is undisputed that he browsed the CD-ROMs containing such software, which action alone, given the circumstances of the case, was extremely serious. It is notable that, in view of his training, the Applicant ought to have known enough to realize that he was imperiling the entire ICTY computer network: a network vital to individual liberties, which could have been stalled or made more vulnerable to

hostile penetration as a result of his repeated actions. The Applicant's case hinges on the fact that no evidence of his intention to use the programs has been put forward, but this, in light of the foregoing, is not relevant.

XV. The Applicant alludes to a Judgement rendered by the Tribunal in 2005 (Judgement No. 1244). The Applicant in that case challenged the Secretary-General's refusal to follow a recommendation of the JDC, which considered the Applicant's conduct to amount to negligence whereas the Secretary-General regarded it as misconduct. The Tribunal found for the Applicant, arguing that the Secretary-General's position was not based on sufficiently relevant facts or proven fraudulent intent to warrant a finding of fraud. It must be pointed out that that case is not germane to the present one inasmuch as the Secretary-General based his decision to dismiss this Applicant not on the existence of a harmful intent constituting a wrongdoing but on his actions alone, which actions posed a threat to the security of the ICTY network as the letter of termination he received makes plain:

“The Secretary-General has examined your case in the light of the JDC's report, as well as the entire record, and the totality of the circumstances. He does not share the JDC's conclusion that your actions did not amount to misconduct and he regrets that he cannot agree with the JDC's assessment of the evidence against you. He considers that the dispositive issue in this case is that you, a telecommunications engineer by background, introduced into the ICTY network your CD-ROMs even though you knew that they contained hacker software designed to attack the network. *It is far less important, whether or not you tried to run the hacker tools*, notwithstanding the confirmation by the manufacturer - not just any expert - of the anti-virus software that you must have tried to launch or copy the hacker software for the anti-virus to be activated. The Secretary-General considers that *the fact alone that you introduced in the ICYY's network hacker software and you knew what those tools could do to the Organization's network* leaves no doubt as to your culpability and has eroded the Organization's trust in you.

As a result, the Secretary-General considers that your conduct amounted to a serious violation of the standards of conduct and integrity expected of staff members of the Organization, and that this misconduct is incompatible with your continued service with the Organization.” (Emphasis added by the Tribunal.)

The Tribunal considers it well within the Secretary-General's authority to determine that the mere fact of loading a personal CD-ROM containing hacker software onto a computer on the ICTY network imperiled that extremely sensitive network, notwithstanding the fact that it has not been definitively shown that an attempt was made to use the software to hack the system, and that such a threat, albeit virtual, to the security of the ICTY network constituted misconduct. That a computer alert prevented the Applicant's actions from disrupting the network or causing security breaches is no reason not to regard his actions as very serious. It is pertinent to recall that the Tribunal has previously held that “serious misconduct is not measured by its consequences but rather by the seriousness of the conduct” (see Judgement No. 1103, *Dilleyta* (2003), para. IX).

XVI. Thirdly, the Tribunal will address the Applicant's claims that he was not accorded fair and equitable treatment during the disciplinary proceedings against him. In so doing, it must ascertain whether there was any procedural irregularity, improper motive or abuse of purpose. Nothing in the Applicant's submissions indicates that he suggests improper motive, abuse of purpose or even arbitrariness towards him. He does, however, assert that he was not properly treated during the proceedings. The Tribunal has carefully considered the development of the

proceedings and believes that the Applicant received due process at every stage: he was informed of the charges against him; he had the assistance of counsel during the proceedings; he attended a video-conference at which he presented his defense; and, he was able to add the opinions of Information Technology experts to the case file, all of which goes to show that his case was attentively examined by the JDC which, in addition, called upon a computer expert in order to enhance its understanding of the technical aspects of the case. The Tribunal thus finds no breach of due process in the proceedings leading to the Applicant's dismissal.

XVII. The Tribunal must finally consider whether this misconduct warranted the Applicant's dismissal - i.e. whether the punishment was proportionate to the offence. Dismissal is, of course, extremely severe punishment. The Tribunal does not, however, consider that it ought to criticize the Secretary-General's decision that the facts warranted the Applicant's dismissal. The position that the Applicant held, that of Security Officer, required him to be especially responsible, which he was not at the time of the computer operations in question, as emphasized by an internal memorandum of 28 March 2003: "The ICTY cannot afford to ignore misconduct of the nature committed by [the Applicant]. The fundamental work of the ICTY is based on confidentiality and security; it cannot permit a Security Officer (who is authorized to carry a weapon) to attempt to breach those without some consequences."

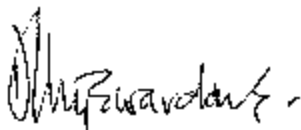
The analogy is particularly striking: who could condone a Security Officer playing with a loaded weapon, even if his intention was not to wound or kill? The same holds true, in the Tribunal's view, of the computer operations in which the Applicant engaged, even if he had no harmful intent, given the dramatic consequences that his actions might have had. While acknowledging that the punishment is severe, the Tribunal agrees with the Secretary-General's argument: in the circumstances, the Applicant's conduct fell markedly short of the standards of conduct and integrity to be expected of every United Nations staff member, and is incompatible with further service with the Organization.

XVIII. In view of the foregoing, the Tribunal finds the Application groundless and rejects all the Applicant's pleas.

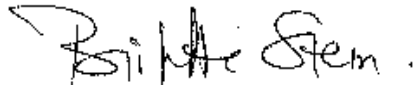
(Signatures)



Spyridon **Flogaitis**
President



Dayendra Sena **Wijewardane**
Vice-President

A handwritten signature in black ink that reads "Brigitte Stern". The letters are cursive and somewhat stylized.

Brigitte **Stern**
Member

Geneva, 27 July 2007

A handwritten signature in black ink that reads "Maritza Struyvenberg". The signature is more fluid and cursive than the one above.

Maritza **Struyvenberg**
Executive Secretary